April 26, 2021

Intel Collaborates with Microsoft against Cryptojacking

Microsoft Defender for Endpoint integrates Intel's silicon-based threat detection to advance endpoint detection and response against cryptojacking malware.

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **What's New:** Starting today, Microsoft Defender for Endpoint expands its use of Intel® Threat Detection Technology (Intel® TDT) beyond accelerated memory scanning capabilities to activate central processing unit (CPU) based cryptomining machine learning (ML) detection. This move further accelerates endpoint detection and response for millions of customers without compromising experience.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20210426005727/en/

By leveraging Intel Threat Detection Technology , Microsoft Defender for Endpoint gains full stack visibility to detect advanced threats, such as cryptojacking, and can remediate the attacks before the user's PC is affected. (Credit: Intel Corporation)

> *"This is a true inflection point for the security industry as well as our SMB, mid-market and enterprise customers that have rapidly adopted Windows 10 with built-in endpoint protections. Customers who choose Intel vPro® with the exclusive Intel® Hardware Shield now gain full-stack visibility to detect threats out of the box with no need for IT configuration. The scale of this CPU-based threat detection rollout across customer systems is unmatched and helps close gaps in corporate defenses."*
> — Michael Nordquist, senior director of Strategic Planning and Architecture in the Business Client Group at Intel

About Intel Threat Detection Technology: Intel TDT, part of Intel® Hardware Shield's suite of advanced capabilities on Intel vPro® and also available on Intel® Core™ platforms, equips endpoint detection and response (EDR) solutions with CPU heuristics for advanced memory scanning, cryptojacking and ransomware detection. With nearly a billion Intel TDT-capable PCs in the market, these are the only CPU-based malware behavior-monitoring capabilities in market that go beyond signature and file-based techniques.

"Intel is unlocking capabilities in its system on a chip that fundamentally change the rules of the game," said Frank Dickson, program vice president of Security and Trust at IDC. "The silicon-level telemetry and functionality enable the hardware compute platform to play an active role in threat defense against 'above-the-OS' attacks. Clearly the goal is to empower Intel®-based systems of today and tomorrow to be fundamentally more secure and have lower malware infection rates than AMD, Apple and other ARM-based processor systems."

Why It Matters: In April 2020, nearly 5,400 cryptocurrencies with a total market capitalization of $201 billion were traded. Since then, the market value has increased as

cryptocurrency is making its way into the mainstream. The financial rewards of cryptocurrency create new threats and risks. As their value rises, cybercriminals shift their focus from ransomware to cryptojacking.

Cryptojacking is malicious cryptomining where cybercriminals install malware into business and personal computers, laptops and mobile devices. This malware uses the computer's power and resources to mine for cryptocurrencies or steal cryptocurrency wallets that can slow computers dramatically and keep them from operating normally. Some cryptojacking scripts have worming capabilities that allow them to infect other devices and servers on a network.

How Intel TDT Works: Intel TDT helps endpoint security solutions harness CPU telemetry and hardware acceleration to help identify threats and detect anomalous activity. It uses a combination of CPU telemetry and machine learning (ML) heuristics to detect specific behavior. The CPU performance monitoring unit (PMU) sits below the applications, operating system and virtualized layers to provide a greater view into active threats across the stack. Intel TDT bolsters EDR solutions and improves visibility where it has historically been a challenge, including the increasing trend of malware attempts to cloak itself in a virtual machine.

“This partnership is one example of our ongoing investment and deep collaboration with technology partners across the industry. We work closely with chipmakers to explore and adopt new hardware-based defenses that deliver robust and resilient protection against cyberthreats,” Karthik Selvaraj, principal security research manager at Microsoft. “As organizations look to simplify their security investments, built-in platform-based security technologies, such as the integration of Intel TDT with Microsoft Defender for Endpoint, combine best of breed in a streamlined solution.”

As threats are detected, Intel TDT sends a high-fidelity signal that triggers remediation workflows of EDR solutions to help protect the infected PC and prevent lateral movement across the corporate fleet. The telemetry and ML heuristics are seamlessly incorporated as part of the endpoint solution and multiple concurrent detectors can run in parallel.

This advanced threat detection doesn’t create a performance hit requiring IT leaders to make a tradeoff between better security or a good user experience. Intel TDT can offload performance-intensive security workloads to the integrated graphics controller and return performance back to the CPU, allowing for increased scanning and reduced impacts to the computing experience.

The threat detection capabilities are native to Intel Core and vPro platforms[1] and operate seamlessly with EDR solutions without the need for installation or deployment IT configuration. When combined with remote monitoring and maintenance, rigorous cybersecurity defenses of Intel Hardware Shield, and no-contact deployment of the 11th Gen Intel® Core™ vPro® mobile processor, customers are assured they have the world’s most comprehensive hardware-based security for business.[2]

More Context: Endpoint Security with Microsoft Defender for Endpoint with Intel TDT (Video) | Intel Provides New Tools to the Cybersecurity Task: The Results Could Be Game Changing, (Frank Dickson and Michael Suby, IDC) |Intel Threat Detection Technology | Intel vPro Platform | Security News at Intel

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

[1] Intel® Threat Detection Technology (Intel® TDT) accelerated memory scanning was first available with 6th gen Intel® Core™ and Intel vPro® platforms. Intel TDT cryptojacking and ransomware detection was introduced with 10th gen and newer Intel Core and Intel vPro platforms.

[2] In thin-and-light Windows-based devices, based on 1) unique features and performance testing on industry benchmarks and Representative Usage Guides across three key usages: productivity, creation and collaboration, comparing Intel® Core™ vPro® i7-1185G7 to AMD Ryzen 7 PRO 4750U and 2) an IOActive study (commissioned by Intel) comparing Intel® Hardware Shield security capabilities on 11th Gen Intel Core vPro processors with corresponding competitor technologies. All testing as of December 2020. Visit www.Intel.com/11thgenvpro for details. Results may vary.

No Product or component can be absolutely secure.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20210426005727/en/

Leigh Rosenwald
1-503-784-7492
leigh.rosenwald@intel.com

Source: Intel